Chapter 1 Reliability Statistics

"There are three kinds of lies: lies, damned lies and statistics."
Benjamin Disraeli (unconfirmed) (1804–1881), British statesman, author.

"Like dreams, statistics are a form of wish fulfillment."
Jean Baudrillard (b. 1929), French semiologist. Cool Memories, ch. 4 (1987, trans. 1990).

Where are we going with this and why is it important?

In this section we are going to relate general statistical theory to specific formulas for calculating reliability. Later in the book we are going to use this foundation for many of the safety system analysis tools. We will simplify some of the material presented here based on assumptions. Also, terms like "Mutually exclusive" have an important meaning when doing things like performing a fault tree analysis.

Introduction

This chapter gives a short introduction to statistics used in safety system reliability analysis. It is not intended to be thorough or generally applicable outside the context of safety systems. One should consult the references for a more thorough treatment of statistics and reliability statistics in particular.

The two quotes at the start of this chapter illustrate that statistics, taken out of context or given incomplete treatment, can lead to unacceptable results. In the world of safety systems, incomplete statistics can lead to under design or over design of safety functions. The former case could lead to accidents, the latter to unacceptable system availability or difficulty in operations.

Safety system design and evaluation involves estimation of both the probable and the possible. Conversely, the compliments of these are the improbable and the (nearly) impossible. Each of these concepts is aided by the use of statistical models to project outcomes of unmitigated and then mitigated risk, the safety system being one form of mitigation.

Probability

A probability is a measure of the chance of the possible outcomes for an event at a given point. The bounds of probability are between zero – not possible, and one – absolute. The sum of all possible outcomes must add up to one. Another way of looking at it is that all possible outcomes must be accounted for. A coin has two sides. We may only be interested in "heads", in our application, but "tails" is the other possible outcome. (This gets us back to the idea of inferred outcomes. We still must account for the fact that the "tails" side exists.) Together the probability of flipping heads and the probability of flipping tails must add up to 1.

Note that probability can only give an insight to the chance of a future event. Once an event has been observed, the probability of a given outcome is unity. For safety systems that may mean the beginning of an incident investigation!

Probability functions describe the chance of a given outcome at a particular point in time. There are two types of probability functions considered here, the discrete probability and the continuous probability. We generally use continuous probability functions to describe the chance of failure of one or more system components. For example, a safety computer has a probability of failure measured in failures per billion hours, termed FITS. A place where we may use discrete probabilities would be to calculate the chance that two out of three safety computers will fail when the accelerator is operating.

P(x) is the probability of a discrete outcome and *f(x)* is the probability density of a continuous function.

$$\sum_{i=1}^{n} P(x_i) = 1 \tag{1.1}$$

for discrete outcomes.

$$\int_{-\infty}^{\infty} f(x)dx = 1 \tag{1.2}$$

for continuously variable outcomes.

Both are read as "the sum total of the probabilities all possible outcomes must add up to 1."

An example of a discrete outcome would be a die toss. There are only six faces on the die. Your chance of getting any one number is 1 in 6 for each toss. An example of a continuous function would be the chance of your car breaking down tomorrow.

Reliability (R) is defined as the *probability that a system will achieve a desired result over a given mission time*. As we will see later, the "desired result" may take on different meanings for a safety system. For example, if a safety system fails safe, the system has achieved the desired result. To the accelerator operator, the safety system has shut down the accelerator – not a desired result in their mind. Put another way, reliability is the probability that a safety function will NOT fail in an unsafe manner over a given time period. In recent treatments this is termed *safety reliability* in order to point out the distinction. This is a book on safety systems so we will interpret reliability and safety reliability to mean the same thing.

In safety systems we are usually interested in the question "what is the probability that a safety system will fail during a specific period of time." In that case we are interested in the cumulative probability of failure or success over a given time interval.

$$F(t) = \int_{t1}^{t2} f(t)dt \qquad (1.3)$$

$$R(t) = \int_{t1}^{t2} [1 - f(t)]dt \qquad (1.4)$$

For accelerators, we are interested in two time ranges – the probability of system failure between certification intervals, and the average probability of failure over the life of the system. For most practical applications *t_1=0 and t_2=t.*

Failure or Hazard Rate

One of the most quoted (and misunderstood) parameters in reliability nomenclature is the failure rate *λ(t)* and this is one place where the system safety and process safety literature differ in treatment of the subject. In reliability engineering texts, it is assumed that if the safety system fails, there is by definition a hazard and the hazard rate *h(t)= λ(t).* In the IEC61508 standards and similar recent treatments mainly from the process industries, failure rates are broken down in to safe failure rates and dangerous failure rates. It is presumed that safe failures will not present a hazard while dangerous (fail-unsafe) failures will.

$$\lambda(t) = \lambda^S(t) + \lambda^D(t)$$

Failure rate is defined as *the probability of failure per unit interval given that the system or component has not failed yet*. Of course, the most commonly used interval is time. However failure rate may be expressed in failure per lot, per demand, per meter, per phase of the moon and so on.

Since the failure rate is probability per unit time, the probability of failure can be expressed as *λ(t)multiplied by a time interval, Δt.*

It is easy to see why the aerospace industry may automatically consider a system failure a hazard. A failure, even a "fail-safe" failure in an aircraft could result in loss of the aircraft and everyone on board. Accelerators have the luxury of being able to shut down in the fail-safe mode without endangering people. This may not be the case for equipment. A beam loss event with a multi-megawatt beam can do considerable damage.

A general discrete expression for failure rate is[1] $\lambda(\Delta t) = \dfrac{N_t - N_{t+\Delta t}}{N_t \Delta t}$ where

N_t = *initial number of units at time t*

$N_{t+\Delta t}$ = *number of units surviving after time Δt*

Normally a constant failure rate is assumed and this is simplified to

$$\lambda = \frac{Number\ of\ \ failed\ \ units}{Total\ number\ of\ units} \cdot \frac{1}{hours\ in\ operation}$$

Example: An accelerator has 50 door interlock switches that were installed 18 years ago. Over that time period, 6 switches have failed unsafe. What is the unsafe failure rate?

$$\lambda^D = \frac{6}{50} \cdot \frac{1}{18 \cdot 8760} = 7.6 \times 10^{-7} \ h^{-1}$$

A more precise expression for *λ(t)* is the probability of failure at time *t* with respect to the probability of survival over a given time interval. As the limit of the time interval approaches zero, the expression becomes:

$$h(t) = \lambda(t) = \frac{f(t)}{1 - F(t)} = \frac{f(t)}{R(t)} \tag{1.5}$$

This is termed the instantaneous failure rate.

Note that for the exponential distribution the hazard rate is constant:

$$f(t) = \lambda e^{-\lambda t} \tag{1.6}$$

$$F(t) = \int_0^t f(t)dt = \int_0^t \lambda e^{-\lambda t} dt \tag{1.7}$$

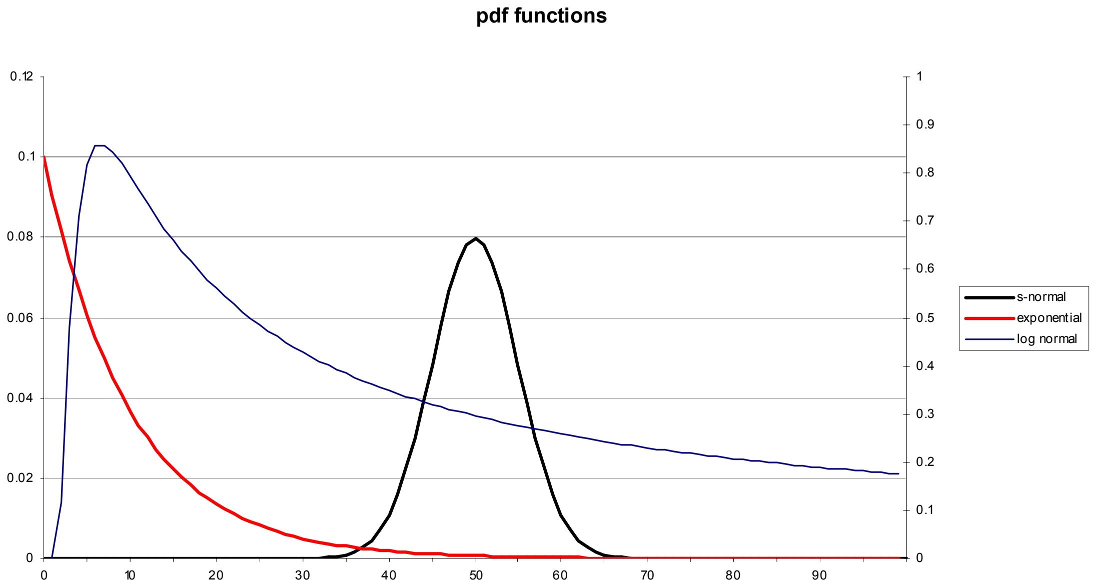
$$F(t) = \frac{-\lambda}{\lambda} e^{-\lambda t} = -e^{-\lambda t} \Big|_0^t = e^0 - e^{-\lambda t} = 1 - e^{-\lambda t}$$

$$R(t) = 1 - F(t) = e^{-\lambda t} \tag{1.8}$$

for the normal distribution

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{\lambda e^{\lambda t}}{e^{\lambda t}} = \lambda \tag{1.9}$$

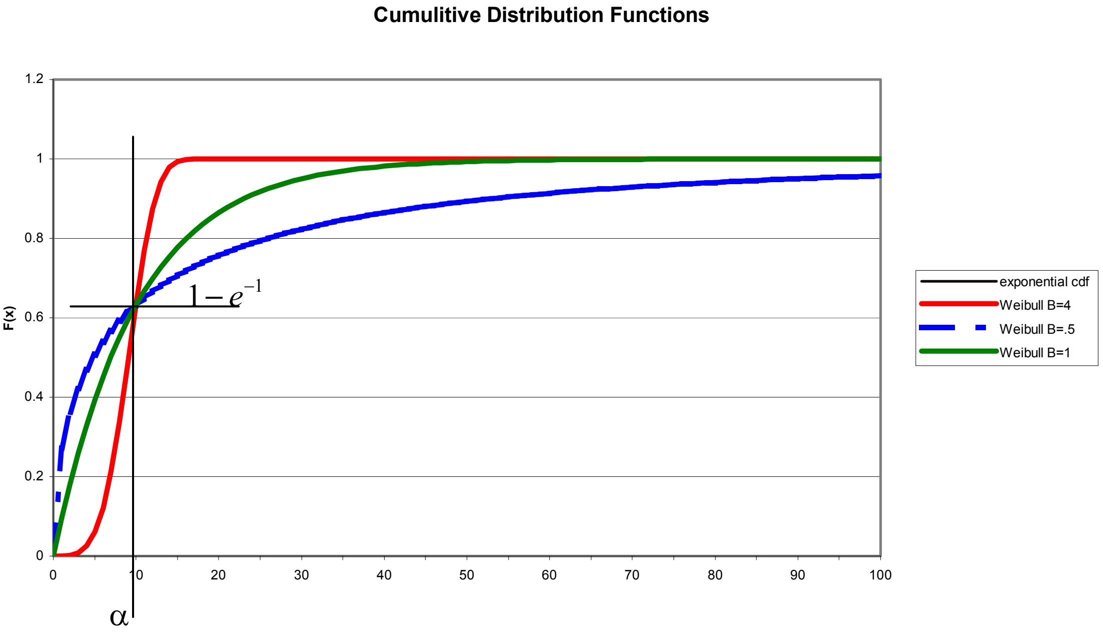
That is, for the exponential distribution, failure rate is not a function of time. This is the most commonly used definition of failure rate. This is also the definition that will be used throughout this book unless otherwise noted. Why? Because it is an expression of failure rate as a function of time that can be easily measured and inserted in to time based reliability models such as the Markov.

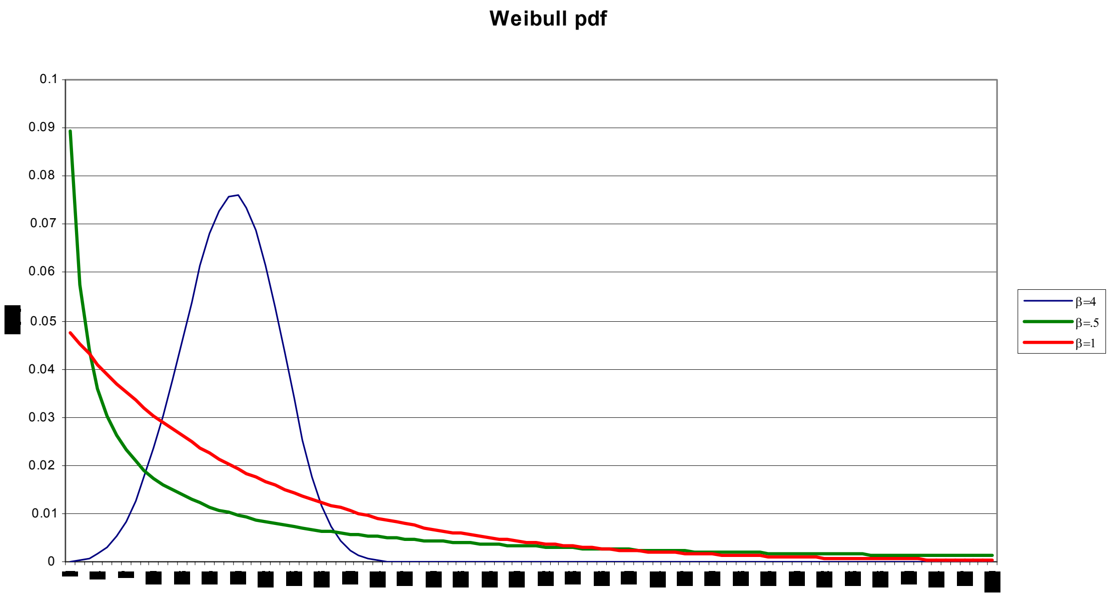


Other

The cumulative hazard function H(t) is:

$$H(t)=\int_0^t h(t)dt=\int_0^t \frac{f(t)}{1-F(t)}dt \tag{1.10}$$





Discrete Statistics

Binomial Distribution *[Rheja, O'Connor]*

The binomial distribution applies to systems where there are mutually exclusive outcomes, e.g. failed or not failed. It can be used to estimate the reliability of redundant or fault tolerant systems.

$$f(x) = \binom{n}{x} R^x (1-R)^{n-x} \tag{1.11}$$

where

$$\binom{n}{x} \rightarrow \frac{n!}{x!(n-x)!}$$

This is the probability that, out of n units, there will be x good ones and n-x bad ones when the probability of having a good unit is R and the probability of having a bad unit is R-1. Note that for binomial distribution, x is an integer.
The mean and standard deviation of the binomial distribution are:

$$\mu = nR \tag{1.12}$$

$$\sigma = \sqrt{nR(1-R)} \tag{1.13}$$

The cumulative distribution function for a binomial distribution is the sum of success states:

$$R(s)=\sum_{i=m}^{n}\binom{n}{m}R^{i}\left(1-R\right)^{n-i} \qquad (1.14)$$

where m is the number of success states out of n total states.

Example.
A safety function uses triplicate sensors. At least 2 of the sensors must be operable for the system to continue to function over the mission time of the system. Each sensor has a calculated reliability of 0.99 over the mission time. What is the probability of system success?

Solution: The system will be successful if at least 2 out of the three sensors are operating, i.e. the success states are 2 out of 3 or 3 out of 3. From equation (1.14), the probability of success over the mission time is:

$$R(r)=\binom{3}{2}(.99)^{2}(.01)^{3-2}+\binom{3}{3}(.99)^{3}(.01)^{3-3}$$

$$=\frac{3!}{2!1!}(.99)^{2}(.01)^{1}+\frac{3!}{3!0!}(.99)^{3}(.01)^{0}$$

$$=3(.99)^{2}(.01)+1(.99)^{3}(1)$$
$$=0.999702$$

	pdf	**CDF Failure**	**Hazard Rate**
s-normal	$f(x)=\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^{2}\right]$	$F(x)=1-\left(\frac{1}{\sigma\sqrt{2\pi}}\int_{x}^{\infty}\exp\left[-\frac{1}{2}\left(\frac{x-\mu}{\sigma}\right)^{2}\right]dx\right)$	$\frac{f(t)}{R(t)}$
log-normal	$f(x)=\frac{1}{x\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{\ln x-\mu}{\sigma}\right)^{2}\right]$	$F(x)=1-\left(\frac{1}{\sigma\sqrt{2\pi}}\int_{x}^{\infty}\frac{1}{x}\exp\left[-\frac{1}{2}\left(\frac{\ln x-\mu}{\sigma}\right)^{2}\right]\right)dx$	$\frac{f(t)}{R(t)}$
exponential	$f(x)=\lambda e^{[-\lambda x]}$	$F(x)=1-\mathrm{e}^{[-\lambda x]}$	λ
Weibull	$f(x)=\frac{\beta\left(x-\gamma\right)^{\beta-1}}{\alpha^{\beta}}\exp\left[-\left(\frac{\left(x-\gamma\right)}{\alpha}\right)^{\beta}\right]$	$F(x)=1-\exp\left[-\left(\frac{x}{\alpha}\right)^{\beta}\right]$	$\frac{\beta}{\alpha^{\beta}}t^{\beta-1}$

Table x. Common continuous probability functions

[1] Rheja pp14